

2013

## **Security without secrecy? Counter-terrorism, ASIO and access to information**

Mark Rix  
*University of Wollongong, [mrix@uow.edu.au](mailto:mrix@uow.edu.au)*

Follow this and additional works at: <https://ro.uow.edu.au/gsbpapers>



Part of the [Business Commons](#)

---

### **Recommended Citation**

Rix, Mark: Security without secrecy? Counter-terrorism, ASIO and access to information 2013, 240-263.  
<https://ro.uow.edu.au/gsbpapers/403>

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: [research-pubs@uow.edu.au](mailto:research-pubs@uow.edu.au)

---

## Security without secrecy? Counter-terrorism, ASIO and access to information

### Abstract

The Foreign Office declined to disclose the reasons for deciding that specific files should be withheld, with the result that the reason for the continuing secrecy is itself ... a secret.

### Keywords

asio, without, information, terrorism, security, counter, secrecy, access

### Disciplines

Business

### Publication Details

Rix, M. (2013). Security without secrecy? Counter-terrorism, ASIO and access to information. In D. Baldino (Eds.), *Spooked: the truth about intelligence in Australia* (pp. 240-263). Sydney, Australia: NewSouth Publishing.

## **Security without Secrecy?**

### **Counter-terrorism, ASIO, and access to information**

The Foreign Office declined to disclose the reasons for deciding that specific files should be withheld, with the result that the reason for the continuing secrecy is itself...a secret.<sup>1</sup>

**Mark Rix**  
**University of Wollongong**

*With more and more secrecy, there is greater security.*

**Misguided and naive.** The idea that providing ASIO, Australia's domestic intelligence (in other words, spy) agency, with greater powers to prevent disclosure about it and its activities makes Australia and Australians more secure from the threat of terrorism has been repeatedly endorsed by successive governments since the attacks on the World Trade Centre and Pentagon in 2001. They have been much more reluctant to explain how secrecy actually adds to security. There can be little dispute with the assertion that some level of secrecy is required by ASIO to enable it to deal effectively with the terrorist threat. It is far more difficult to accept that complete secrecy, and no accountability, equates to water-tight security. Before considering these issues in greater depth, a couple of brief case studies will set the scene for the investigation to follow.

#### **A couple of preliminary case studies**

Intelligence agencies', police forces', public officials', governments' justification for keeping secret the reasons for not disclosing what they regard as secrets captures the central conundrum of this chapter. The reasoning is really quite simple: there can be no security without secrecy. Seldom is evidence adduced to support this line of reasoning because, if the reasoning is accepted as justified, it would breach and weaken security. A relevant case, now some years old, illustrates the point that is being made here. The second, more recent case perhaps makes the same point even more resoundingly.

Izhar Ul-Haque, then a Sydney medical student, was charged with training with the Pakistan-based terrorist group Lashkar-e-Toiba in 2003 well before it had been classified as a terrorist organisation by the United Nations. On November 5<sup>th</sup> 2007 in the NSW Supreme Court, Justice Michael Adams found that all records of interview with Mr Ul-Haque tendered by the Australian Federal Police as evidence were inadmissible forcing the NSW Director of Public Prosecutions to withdraw the case just before a jury was empanelled.<sup>2</sup> The AFP had also tried to elicit information from Mr Ul-Haque about the terror suspect Faheem Lodhi by questioning him in a maximum security gaol for more than two hours but without first cautioning him or informing his lawyer of the interrogation.<sup>3</sup> Two AFP officers had demanded that Mr Ul-Haque turn informant against Lodhi who was subsequently convicted and gaoled for 20 years for conspiring to bomb the national electricity grid.<sup>4</sup> When he

refused to do so, Mr Ul-Haque was threatened that there would be serious and adverse consequences for him.

While Mr Ul-Haque had briefly trained with Lashkar-e-Toiba in early 2003, the law enforcement authorities had admitted to him that they accepted his connection to the organisation had nothing to do with Australia but instead was because of his opposition to the Indian presence in Kashmir. The AFP records of interview were found to be inadmissible because of the improper and oppressive conduct of the AFP (and ASIO) officers involved, and because of the inextricable links between AFP and ASIO including the disclosure by the AFP to ASIO of what Mr Ul-Haque had said in interview. Justice Adams also found that two ASIO officers (whose identities remain secret) had committed the criminal offences of kidnapping and false imprisonment at common law and another offence under the Crimes Act. He also found that the conduct of the ASIO officers amounted to a gross breach of the powers they had been granted under the search warrant which had been issued to them.

Ian Carnell, then Inspector-General of Intelligence and Security, found in his subsequent report of ASIO's actions in the case, contrary to Justice Adams' conclusion, there were insufficient grounds for referring the matter for prosecution. He also concluded that there was insufficient evidence to support compensation to Mr Ul-Haque for false imprisonment.<sup>5</sup>

The recent Ben Zygier, or 'Prisoner X, case in which ASIO was somehow involved is in its own way even more perplexing than Izhar Ul-Haque's. Trying to figure out exactly what went on is like trying to find your way in the dark in unfamiliar territory without a torch such is the secrecy surrounding the case that is being maintained by both Israel and Australia. Mr Zygier, a dual Australian-Israeli citizen, was found dead in December 2010 in his 'suicide-proof' prison cell in Israel's maximum-security Ayalon prison. He is believed to have hanged himself with a bed sheet. Evidently, he had been detained by the Israelis for serious breaches of that country's security laws. These breaches allegedly involved passing information to ASIO about Mossad's practice of using Australian passports to enable its agents to spy in countries that are hostile to Israel. The Israeli Prime Minister, Benjamin Netanyahu has denied that Zygier passed on information to any Australian security agency, specifically ASIO. Australian Attorney-General Mark Dreyfus backed up this claim. Much more seriously for Zygier, he unintentionally sabotaged a highly sensitive and secretive Mossad operation to repatriate the remains of Israeli soldiers killed in the 1982 war in Lebanon. For this he was evidently charged with treason.<sup>6</sup>

## **Introduction**

After the 11 September 2001 terrorist attacks in the US, Australia became a particularly

active combatant in the ‘war on terror’ especially in the field of legislation with what Professor George Williams referred to on the 10<sup>th</sup> anniversary of ‘9/11’ as an ‘extraordinary burst of law-making’.<sup>7</sup> Its legislative performance has eclipsed the relatively paltry efforts of Great Britain, the United States and Canada not only in purely quantitative terms but also in the extent to which these efforts have gone in inhibiting the liberties and rights of every Australian. Misuse and abuse of information, inscrutable but far-reaching information classification procedures and downright obfuscation all have become key weapons in the counter-terrorism arsenal of democratically-elected governments like Australia’s. Indeed, it seems at times to be a war on openness and accountability rather than terror such are the curbs on transparency and public disclosure that have been introduced since 11 September 2011. Australia has led the field in this particular campaign.

This chapter is primarily concerned with investigating the Australian Security Intelligence Organisation’s role in the protection of Australia’s national security in what was at least until 2009 (when the phrase was abandoned by the Obama Administration, a decision renewed in May 2013) known around the world officially and unofficially as the global ‘war on terror’. In addressing this primary concern, the chapter will consider the powers that ASIO is granted under the Australian Security Intelligence Organisation (ASIO) Act 2003, in particular, ASIO’s sweeping questioning and detention powers and the severe restrictions the Act imposes on suspects, and non-suspects, regarding disclosure of information about their questioning and detention by ASIO.<sup>8</sup> The ASIO Act’s restrictions on disclosure of information will be considered with reference to the strict, and complementary, controls on disclosure of ‘information’ or ‘national security information’ in Commonwealth criminal and civil trials that are imposed by the National Security Information (Criminal and Civil Proceedings) Act 2004. The NSI Act, which as will be seen uses the ASIO Act’s definition of what Australia’s ‘security’ comprises, puts considerable obstacles in the way of the chances of a terrorism suspect receiving a fair trial. More importantly for this chapter, the NSI Act erects around terrorism cases an almost impenetrable shield of secrecy and lack of transparency, binds the processes for classifying and protecting information in obscure and unfathomable red (more correctly, invisible) tape, and effectively protects the political executive and national security agencies like ASIO from external, independent scrutiny.

In addition to these two acts, the chapter will briefly consider the Public Interest Disclosures Bill that was introduced into the Federal Parliament by Attorney-General Mark Dreyfus in

March 2013. This Bill feigns, amongst other things, to make it easier to disclose and investigate wrongdoing and maladministration in the Commonwealth public sector. More simply, it will according to Mr Dreyfus and its other proponents in the government legalise public interest whistleblowing. However, like the ASIO and NSI Acts, the Public Interest Disclosures Bill reverts to the default option of a smug but defensive presumption in favour of not disclosing much if any information about defence, security, counter-terrorism or anything else that could conceivably be linked to Australia's 'national security'. As with the ASIO and NSI Acts, the term 'national security' is circularly defined to include 'national security information' (or, 'intelligence information') which is in turn defined to include 'national security'.

Together, these three acts have the effect of creating a sort of three-sided hall of mirrors in which each act's restrictions on the disclosure, and availability, of information are tightened as one act reinforces the other in providing fewer and narrower avenues for access to and release of information in the conduct of terrorism investigations and any subsequent trials. Indeed, it seems that the three acts are all indeed predicated on the assumption that there can be no security without secrecy; in other words that, in effect, secrecy and security are to be equated with each other and each reducible to the other. This is a very dangerous assumption to proceed on not only in counter-terrorism cases or but also in criminal cases of other sorts if democracy, human rights and the rule of law are to have real, practical meaning and effect in this country but especially in the way this country's criminal justice system operates.<sup>9</sup> Whether or not the three acts, individually or in conjunction, actually protect and strengthen Australia's national security in the 'war on terror' is also impossible to determine because of the unavailability of the type of information—that is, information which is comprehensive, independent, and reliable—required by an average individual to enable them to make a well-informed assessment of the acts' effectiveness in this area. Because of this troubling dearth of openness, transparency and accountability, it is simply not possible to reach the conclusion that the established legislation, namely the ASIO and NSI Acts, must be effective because so far as we know Australia has not yet been the victim of a major or even minor terrorist attack.

The absence of evidence in support of the assumption that there is no security without secrecy admittedly does not constitute compelling grounds for rejecting it. More obviously, of course, absence of evidence delivers no compelling grounds for accepting the assumption. In light of this pervasive uncertainty, faith and trust in the integrity of Australia's political

and criminal justice system, its traditions, history, the government, or even its politicians is a possible recourse but if adopted any faith would be blind and the trust largely unfounded. In other words, without accountability and transparency faith and trust are baseless except for the similarly groundless faith and trust that they are in the circumstances the most appropriate or realistic response. And, perhaps more to the point, without openness, transparency and accountability there is can be real security.

In light of the foregoing, it appears that there are a number of alternative ways of framing the chapter's title. Clearly, the most obvious alternative is 'Can there be security without transparency and accountability?' Nearly as obvious contenders are 'Can there be security with transparency and accountability?' and, perhaps the most challenging of the possibilities but too easily dismissed as oxymoronic, 'Can there be security with secrecy but no transparency and accountability?' Challenging and an evident oxymoron it might be, but an affirmative answer to the latter alternative has been and continues to be the default option for Australian governments and the defence, intelligence, security and law enforcement departments, agencies and public servants they claim to oversee. This perhaps obscure and cryptic point will become clearer in the course of the investigation of the counter-terrorism legislation that will be conducted below.

### **The Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003**

The Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003 (Cth) (sometimes referred to as the ASIO Amendment Act 2003 but hereafter simply and generally referred to as the ASIO Act) was introduced into the Commonwealth Parliament during 2003 and enacted later that year. It does not help that the original ASIO Act (1979, Cth) was amended twice during 2003, but every effort here will be made to keep things as clear and straightforward as possible.<sup>10</sup> One of the key amendments was the introduction of Part III Division 3 Special powers relating to terrorism offences often referred to as the 'Special Powers Regime') that 'created a new system of warrants which, when issued, empower [ASIO] to question and detain individuals for the purposes of gathering intelligence about terrorism offences'.<sup>11</sup> The system of warrants is also referred to as the 'Special Powers Regime'. This regime is regarded as 'one of the most controversial pieces of legislation ever passed by the Commonwealth Parliament' because of the 'vesting of "policing" powers of questioning and detention in a domestic intelligence agency.'<sup>12</sup> Initially,

a sunset clause was to have seen ASIO's special powers expire in 2006, but this was subsequently extended out to 2016 (affirmed in the ASIO Legislation Amendment Bill 2006). The amended ASIO Act 2003 extended the questioning period to 48 hours (from 24 hours) if an interpreter is required to be present at any stage of the interrogation of a suspect (or, non-suspect). A person requiring an interpreter cannot be questioned for more than a total of 24, 32 or 40 hours 'unless the prescribed authority before whom the person was being questioned just before the duration of that questioning reached that total permits the questioning to continue'.<sup>13</sup> However, under the Special Powers a person can be detained for up to 168 hours (7 days) whether or not they need an interpreter.

It is important to be clear on the circumstances in which under the ASIO Act a person can be taken into custody, detained and questioned. The relevant Minister (i.e., the Federal Attorney-General) can consent to a request from the Director General of ASIO for a questioning and detention warrant to be issued if he or she has reasonable grounds for believing that this will 'substantially assist the collection of intelligence that is important in relation to a terrorism offence' and 'that relying on other methods of collecting that intelligence would be ineffective'.<sup>14</sup> Thus, a person can be detained without charge, and does not even have to be suspected of having committed any offence (terrorism or other) to be taken into custody and questioned in secret. While being interrogated, a person held in detention has to answer all questions and provide all the information or the 'record' or 'thing' requested of them. A detainee also has to prove that they do not have the information or record or thing requested. If the detainee is unable to do so and does not provide the information, record or thing requested they can be imprisoned for up to five years. A person can also be detained if there are reasonable grounds for believing that if they are not immediately taken into custody they could alert someone who is in the act of committing a terrorism offence that the offence is being investigated, that they might not come before the prescribed authority or that they could 'destroy, damage or alter a record or thing the person may be requested in accordance with the warrant to produce'.<sup>15</sup>

The secrecy provisions are lengthy and incredibly detailed but sections of them are worthy of some attention. These provisions are found in the ASIO Legislation Amendment Act 2003, no. 143, Schedule 1, Part 4 Secrecy relating to warrants and questioning. Before the expiry of a warrant, a person (known as the 'discloser') commits an offence if the 'discloser discloses (*sic*) information' and the information is about the issuing of the warrant, the content of the warrant or the questioning or detention of a person under the warrant and/or the information



is ‘operational information’. Operational information is information that ASIO has or had, a source of information that ASIO has or had (other than the person who is the subject of the warrant), or an ASIO operational capability, method or plan. Even in the 2 years after the expiry of a warrant, it is an offence for a discloser to disclose information when the information is operational information and/or the information has almost anything else to do with the warrant. In addition to these restrictions and prohibitions, what is known as ‘strict liability’ applies if the information is operational information or is about the warrant or the questioning and detention of the person who is the subject of the warrant. It also applies if the discloser is the person whose is the subject of the warrant, or is a lawyer acting for that person who was present during questioning or was otherwise involved in representing the person and knew something about the warrant and how they were treated.<sup>16</sup>

The Special Powers Regime has a tightly limited provision for a person who is questioned and/or detained under a warrant to contact a lawyer of his or her or own choice but the prescribed authority can impose further strict controls on this contact. If, for the example, the prescribed authority is satisfied that contact with the lawyer of the person’s choice may lead to the destruction or damaging of a thing or record associated with the warrant he or she can limit or even prevent contact with the lawyer. And, as the Law Council of Australia points out, the Special Powers enable a person under a warrant to be questioned without a lawyer of the person’s choice being present. The prescribed authority can also ask for the removal of the lawyer during questioning if he or she believes the lawyer is being unduly disruptive. In addition, ‘Section 34L of the *ASIO Act* compels a person named in a warrant to give information and items [thing or record] to ASIO regardless of whether doing so might tend to incriminate the person or make them liable to a penalty.’<sup>17</sup>

The National Security Information Act, which will be considered further below, also imposes restrictions on a lawyer’s access to relevant information. These reinforce and complement the restrictions contained in the ASIO Act. While there is not the scope here to consider the NSI Act’s restrictions on a lawyer’s access to information in great detail, the restrictions imposed by the Act on a defendant’s choice of a legal representative are nevertheless relevant and worthy of some attention. These restrictions are contained in Section 39 of the NSI Act, Security clearances required in federal criminal proceedings. This Section deals with a situation in which a defendant’s legal representative, or person assisting the legal representative, has been notified by the Secretary of the Attorney-General’s Department that

it is probable that in the proceeding a disclosure of information which is likely to prejudice national security will be made.<sup>18</sup> When thus notified a person ‘may apply’ for a security clearance ‘at the level considered appropriate by the Secretary in relation to the information [likely to be disclosed in the proceeding]’.<sup>19</sup>

The level of security clearance required by a legal representative is calibrated to match the highest level of classification of the NSI information that is likely to be disclosed. Classifications of NSI Information range from ‘restricted’, followed by ‘confidential’, then up to ‘secret’ and finally ‘top secret’. So if ‘Secret’ is the highest NSI classification for the information likely to be disclosed then a ‘Secret’ level security clearance is required by the legal representative. The process of classifying information, and of determining the level of its classification, is clouded in secrecy and is evidently a completely arbitrary one; no light at all is thrown on the process by the Act itself including its accompanying Requirements and Regulations or by the *Practitioner’s Guide*. Secrecy and arbitrariness accordingly also surround the process of setting the level of and issuing a security clearance. Nevertheless, as the NSI Act *Practitioner’s Guide* reassuringly points out, ‘The security clearance process is conducted at arm’s length from the agencies involved in prosecutions.’<sup>20</sup>

But what, after all, is ‘information’, what is ‘national security information’, what are ‘security’ and ‘national security’ and what is national security information, specifically, that which is ‘likely to prejudice national security’. The section below, which considers the NSI Act and its relationship with the ASIO Act, attempts to cast some light on these unnecessarily obscure terms and the phenomena they denote. This is not as easy as it would first seem because attempting to cast light involves entering another hall of mirrors.

### **The National Security Information (Criminal and Civil Proceedings) Act 2004**

The NSI Act and the ASIO Act together set the conditions under which information in counter-terrorism cases can be accessed and used by lawyers, journalists, members of the public or any other interested parties. The object of the NSI Act is to prevent the disclosure in Federal criminal or civil proceedings of information that is likely to prejudice national security ‘except to the extent that preventing disclosure would seriously interfere with the administration of justice.’<sup>21</sup> In defining ‘information’ the NSI Act defers to the Commonwealth Criminal Code. In the Code (subsection 90.1(1)) information is defined as meaning ‘information of any kind, whether true or false and whether in material form or not, and includes a) an opinion, and b) a report of a

conversation.’<sup>22</sup> The NSI Act supplements this already far-reaching and all-encompassing definition with the phrase ‘whether or not in the public domain’. Thus, in the end, information can be very nearly anything and the term is accordingly vacuous and meaningless. But, the point is of course that the breadth, meaninglessness and vacuousness of the term provide the government, and ASIO, with an almost impenetrable and unfathomable legislative screen for hiding information and tightly controlling its use and disclosure even in circumstances where this is prejudicial to a terrorism suspect’s chance of receiving a fair trial. Indeed, non-disclosure of any information by anyone seems very much to be the preferred option. Not only does this prejudice the chance of a fair trial for a suspect, it is also completely prejudicial to democratic accountability and transparency. The definition of ‘national security information’ provided by the Act, which is considered below, does not improve the situation. Before looking at this definition, however, the meaning of ‘national security’ and the other terms contained in it first have to be considered.

As the Act’s *Practitioner’s Guide* redundantly points out, ‘The meaning of “national security” is central to the operation of the NSI Act, Regulations and Requirements.’<sup>23</sup> In the Act (Section 8) ‘national security means Australia’s defence, security, international relations or law enforcement interests.’ The meanings of these other terms, which are defined in turn, make national security even broader and more inclusive than it already is. ‘Law enforcement interests’ are defined to include foreign and security intelligence, and the technologies and methods used in its collection, analysis and security, within its ambit. These interests have been included in the definition of ‘to ensure that law enforcement information which is connected to national security...is not excluded from protection under the NSI Act.’<sup>24</sup> The Act adopts the same definition of ‘security’ as that contained in Section 4 of the ASIO Act 1979 where security means the protection of Australia and Australians from espionage, sabotage, politically motivated violence and the promotion of communal violence, attacks on the country’s ‘defence system’ and foreign interference whether these are ‘directed from, or committed within, Australia or not’. To this sweeping definition is added ‘the carrying out of Australia’s responsibilities to any foreign country’ in relation to any of these matters.<sup>25</sup>

Not surprisingly, in addition to defining ‘national security’ (and the various terms other than defence embedded in it) and ‘information’, the NSI Act defines ‘national security information’ to be a sort of supplement to the definitions of these other two terms ensuring that each is inseparably tied to the other.<sup>26</sup> Building on the object of the Act, ‘national security information’ is information that either ‘relates to national security’ or ‘the disclosure of which may affect

national security.’ ‘Relates to’ and ‘may affect’ are not further defined or explained. Nevertheless given the broad meaning of national security and information, almost any conceivable information (even that which is inconceivable or non-information) either actually or potentially relates to or affects national security. However, the *pièce de résistance* in the NSI Act lexicography is ‘prejudicial to national security’ the definition of which is so utterly circular as to mean almost nothing (and, therefore nearly everything). The meaning of this term is provided in Section 17, where it is defined thus: ‘1) A disclosure of information is *likely to prejudice national security* if there is a real, and not merely a remote, possibility that the disclosure will prejudice national security.’<sup>27</sup>

Despite the evident meaninglessness, vacuousness and circularity of these terms they can have very important and very serious effects for a defendant when invoked in terrorism trials. Section 24 of the NSI Act requires the Attorney-General to be notified if the information or its disclosure relates to or may affect national security. Where the Attorney-General determines that disclosure of the information would prejudice national security, he or she issues a non-disclosure certificate to the court (Section 26). It is not clear how such a determination is arrived at by the Attorney-General. In any event, there are different sorts of certificates that can be issued by the Attorney-General if he or she has decided that information prejudicial to national security is likely to be disclosed in criminal (or, civil) proceedings. A criminal non-disclosure certificate is issued when the Attorney-General has been notified under Section 24 or subsection 25(6) that information relating to or which could affect national security will be disclosed by a party to the proceeding or a witness and he or she believes that the information is likely to prejudice national security. The Attorney-General issues a criminal witness exclusion certificate when he or she has been notified under Section 24 or 25(6), or expects ‘that a person whom the prosecutor or defendant intends to call as a witness may disclose information by his or her presence’ and believes that this information is likely to be prejudicial to national security.<sup>28</sup> Naturally, a defendant can appeal against the issuing of a criminal non-disclosure or witness exclusion certificate. However, ‘the court is required to give greatest weight to the question of “the risk of prejudice to national security” rather to the needs and rights of the accused’.<sup>29</sup> This is consistent with other aspects of the NSI Act and, as seen above, of the ASIO Act. Worryingly, the new Public Interest Disclosure Bill also shares some of the same aspects.

### **Public Interest Disclosure Bill**

As was noted at the beginning of this chapter, in March 2013 Attorney-General Mark Dreyfus announced that the Public Interest Disclosure Bill, under which public sector whistleblowers will

have more protection, had been introduced to Parliament. According to Mr Dreyfus, the Bill 'reaffirms the Government's commitment to a culture of disclosure in the Australian public sector.' It includes a framework for the investigation of public interest disclosures, whistleblower protections and sets out circumstances in which disclosures can be made outside government. The Attorney-General also pointed out that 'Open and transparent government is a key feature of a strong democracy and this bill, along with our reforms to FOI laws, will help build and maintain that culture'.<sup>30</sup>

The Objects of the Bill are all highly laudable: promoting the integrity and accountability of the Commonwealth public sector; encouraging and facilitating the making of public interest disclosures by public officials; ensuring that public officials who make such disclosures are supported and protected from adverse consequences that may arise from disclosures; and, ensuring that disclosures are properly investigated and dealt with.<sup>31</sup> However, these objects have pretty strict limits which are to be found scattered at various points through the act. For example, it is noted in Division 2, Section 26 in which, amongst other things, public interest disclosures are defined (this definition runs for several pages) that the limitations which should be taken into account in making disclosures are designated publication restrictions and the need to protect intelligence information. Among the several meanings of designated publication restriction is an order under sections 31 or 38L of the NSI Act dealing respectively with non-disclosure certificate and witness exclusion certificate hearings in federal criminal proceedings and civil non-disclosure certificate and civil witness exclusion certificate hearings in civil proceedings. Included in intelligence information is information identifying 'a person as being, or having been, an agent or member of the staff (however described) of the Australian Secret Intelligence Service or the Australian Security Intelligence Organisation.'<sup>32</sup> Intelligence information also includes sensitive law enforcement information which is identical in meaning to the meaning of law enforcement interests included in the NSI Act's definition of national security. Sensitive law enforcement information and law enforcement interests both comprise, amongst other things, foreign and security intelligence, and the technologies and methods used in its collection. Division 29, Section 29 of the Public Interest Disclosure Bill defines and gives examples of different kinds of disclosable conduct (this also runs for several pages). Section 33 deals with Conduct connected with intelligence agencies. There it is stipulated that 'conduct is not *disclosable conduct* if it is: a) conduct that an intelligence agency engages in the proper performance of its functions or the proper exercise of its powers; or b) conduct that a public official who

belongs to an intelligence agency engages in for the purposes of the proper performance of its functions or the proper exercise of its powers.’<sup>33</sup> The Public Interest Disclosures Bill does not deal in detail with information or how it is to be protected, because these, as seen above, are already fully covered in the NSI Act, and in the ASIO Act.

The Public Interest Disclosure Bill passed largely unannounced and unnoticed into law in June 2013. It is a potentially important piece of legislation that seeks to protect from dismissal, retaliation or adverse cost decisions Commonwealth public sector whistleblowers who disclose corruption, fraud and misconduct, and other forms of serious wrongdoing. Unfortunately however, and as noted above, whistleblowing about federal politicians and intelligence agencies is not included in the Act. In other words, Australian incarnations of the likes of Edward Snowden and Bradley Manning would receive no protection under the Act.<sup>34</sup>

## Conclusion

The secrecy surrounding information, national security information, security, national security, international relations, and law enforcement interests is baffling, all-pervasive and largely impenetrable. Successive Australian governments have successively added to this secrecy and impenetrability. It is far less clear whether this has helped to make Australians more secure from the threat of terrorism. It is clear, however, that it has left them more vulnerable to the secret, clandestine and sometimes illegal activities of ASIO which, surrounded in secrecy founded on sloppy, all-encompassing and unfathomable legislation, is subject to few if any requirements for openness, transparency and accountability. In the end, this can only lead to one conclusion: there really is no security in secrecy.

---

<sup>1</sup> Ian Cobain, Richard Norton-Taylor, ‘Files on colonial crimes still kept secret’, *The Guardian Weekly*, 3-9 May 2013. The files relate to events in the final years of the British empire (generally the late 1950s, early 1960s) and deal, amongst other things, with the Mau Mau insurgency in Kenya.

<sup>2</sup> R v Ul-Haque [2007] NSWSC 1251. Available at: <http://www.lawlink.nsw.gov.au/scjudgments/2007nswsc.nsf/aef73009028d6777ca25673900081e8d/d9a9080227820bddca257389007c91e4?OpenDocument>.

<sup>3</sup> Natalie O-Brien, ‘Share intelligence or repeat Ul-Haque debacle’, *The Australian*, 28 February 2008. Available at: <http://www.theaustralian.com.au/news/share-intelligence-or-repeat-ul-haque-debacle/story-e6frg6o6-1111115664280>.

<sup>4</sup> The NSW Court of Criminal Appeal quashed Lodhi’s appeal against his conviction, a ruling subsequently upheld by the High Court of Australia.

<sup>5</sup> Inspector General of Intelligence and Security, Report of Inquiry into Actions taken by ASIO in 2003 in Respect of Mr Izhar Ul-Haque and Related Matters. Available at: [http://www.igis.gov.au/inquiries/docs/ul\\_haque\\_asio\\_2003.pdf](http://www.igis.gov.au/inquiries/docs/ul_haque_asio_2003.pdf).

<sup>6</sup> Ruth Pollard, ‘Israel denies “Prisoner X” Zygier was in contact with ASIO’, *The Sydney Morning Herald*, 20 February 2013; Tom Allard, ‘Israeli intelligence told Australia Zygier was in jail’, *The Sydney Morning Herald*, 23-24 February 2013; Trevor Bormann, ‘Prisoner X sabotaged Mossad operation’, ABC-TV Lateline, 7 May

---

2013: available at: <http://www.abc.net.au/lateline/content/2013/s3754144.htm>; Mitchell Nadin, 'Ben Zygier was accused of treason after compromising a Mossad operation', *The Australia*, 8 May 2013.

<sup>7</sup> George Williams, 'The laws that erode who we are', *The Sydney Morning Herald*, 10 September 2011.

<sup>8</sup> It could be argued that ASIO has been misnamed and that it should have instead been called the Australian Intelligence Security Organisation. Even though this would have more accurately reflected what are evidently ASIO's overriding purposes and objectives, namely the security of intelligence, it would have produced an acronym (AISO) that doesn't nearly as easily roll off the tongue as 'ASIO' does.

<sup>9</sup> Some of these issues are considered, from a prosecutor's point of view, in Chris Craigie (former Commonwealth Director of Public Prosecutions), 'Management of lengthy and complex counter terrorism trials: An Australian prosecutor's perspective', Criminal Justice in Australia and New Zealand: Issues and Challenges for Judicial Administration Conference, 8 September 2011. Available at: <http://www.cdpp.gov.au/Director/Speeches/20110908cc-Management-of-lengthy-and-complex-counter-terrorism-trials.aspx>. Craigie comments (p. 7) 'The involvement of security agencies in these matters [counter terrorism investigations and prosecutions], and the perennial concerns regarding possible disclosure of their methods, capabilities and people, adds a degree of complexity to these matters, particularly given the tension between those security imperatives and the noble common law tradition of natural justice manifested in an open and fair trial.' For a public defender's perspective, see Dina Yehia, "'Being alert and alarmed when acting for those accused of terrorism offences": Consideration of areas of legal and practical difficulties', The Public Defenders Annual Criminal Law Conference, 27 & 28 March 2010. Available at: <http://www.publicdefenders.lawlink.nsw.gov.au/agdbasev7wr/pdo/documents/pdf/terrorismlaws.pdf>.

<sup>10</sup> The first of these is the ASIO Legislation Amendment (Terrorism) Act 2003, no. 77 which was assented to on 22 July. Available at: <http://www.comlaw.gov.au/Details/C2004A01162/>. The second is the ASIO Legislation Amendment Act 2003, no. 143, assented to on 17 December. Available at: <http://www.comlaw.gov.au/Details/C2004A01228>. It is important to realise that acts like the ASIO Act are always subject to further amendment. Thus, on 5 July 2011 then Attorney-General Robert McClelland proudly announced the passage of the Intelligence Services Legislation Amendment Bill through Parliament. Amongst other things, this Act amended the ASIO Act (it also amended the Intelligence Services Act 2001 and the Criminal Code Act 1995) to align the meaning of 'foreign intelligence' in the ASIO Act with the meaning in other acts and to clarify that ASIO computer access warrants authorise ASIO to access data held in a target computer at any time during the life of the warrant. The former of these amendments expands the criteria enabling ASIO to collect foreign intelligence to include Australia's national security, foreign relations and national economic well-being. It also redefines 'foreign power' to become the nebulous and wide-ranging 'people, organisations and governments outside Australia'. See Bernard Keane, 'New powers mean ASIO could spy on WikiLeaks', *Crikey*, 20 May 2011. Available at: <http://www.crikey.com.au/2011/05/18/new-powers-mean-asio-could-spy-on-wikileaks/>. In March of the same year, as Keane reports, the smooth passage of the Telecommunications Interception and Intelligence Services Legislation Amendment Act through both Houses of the Federal Parliament greatly expanded ASIO's power to share information from wiretaps and computer access with other agencies such as ASIS.

<sup>11</sup> Nicola McGarrrity, Rishi Gulati and George Williams, 'Sunset Clauses in Australian Anti-Terror Laws', *Adelaide Law Review*, 33, 2012, p. 309

<sup>12</sup> *Ibid*, pp. 312-313

<sup>13</sup> ASIO Legislation Amendment Act 2003 (no. 143), Section 34HB Time for questioning through interpreter. A 'prescribed authority' is a person 'who has served as a judge in one or more superior courts for a period of 5 years and no longer holds a commission as judge of a superior court.' Amongst others who can be appointed as a prescribed authority, in the event that no one else suitably qualified can be found, are the President or the Deputy President of the Administrative Appeals Tribunal. A prescribed authority is to be distinguished from an 'issuing authority', that is, a person who issues a questioning, detention or questioning and detention warrant. An issuing authority can be a Federal Magistrate or Judge.

<sup>14</sup> ASIO Legislation Amendment (Terrorism) Act 2003 (no. 77), Section 34C Requesting warrants.

<sup>15</sup> *Ibid*. At about 5pm on 14 May 2013 (the same day that the 2013/2014 Federal Budget was brought down), the Government tabled the 2011/2012 Report of the Independent National Security Legislation Monitor (declassified version) in the Federal Parliament. The Monitor (Mr Brett Walker QC) recommended that ASIO's detention warrants be repealed, that the process for issuing ASIO questioning warrants be strengthened and that the control order and preventative detention order regime (not considered in this chapter) be scrapped. The Monitor's report is available at: [http://www.dpmc.gov.au/inslm/docs/INSLM\\_Annual\\_Report\\_20121220.pdf](http://www.dpmc.gov.au/inslm/docs/INSLM_Annual_Report_20121220.pdf). The Monitor had handed his Report to the Government in December 2012. Also tabled in Parliament on 14 May was the Council of Australian Governments Review of Counter-Terrorism Legislation. The COAG Review recommended the repeal of the offence of associating with a terrorist organisation, narrowing the criteria for

banning a terrorist organisation, and tightening some terrorist offences. However, the Review also recommended keeping control orders but with important additional safeguards. The COAG Review is available at: <http://www.coagctreview.gov.au/Report/Documents/Final%20Report.PDF>. See also Jessica Blackbourn and Nicola McGarrity, 'Our excessive anti-terrorism laws must go', *The Drum Opinion*, 15 May 2013 (available at: <http://www.abc.net.au/unleashed/4691190.html>) and George Williams, 'Action on inept anti-terror laws must get priority', *The Sydney Morning Herald*, 21 May 2013.

<sup>16</sup> ASIO Legislation Amendment Act 2003 (no. 143), Section 34VAA Secrecy relating to warrants and questioning. According to the Commonwealth Criminal Code, from which it is drawn, 'The defining features of strict liability are the absence of any requirement of fault, whether for all or some of the physical elements of an offence, coupled with the provision of the defence of reasonable mistake of fact.' Otherwise, the fault element of 'recklessness' applies. According to the Criminal Code a person can be reckless with respect to a circumstance or a result and is aware of the 'substantial risk' that the circumstance exists or will exist and that the result will occur and having regard to these known circumstances unjustifiably takes the risk anyway. This information about the Criminal Code comes from the Attorney-General's Department, *The Commonwealth Criminal Code: A Guide for Practitioners*. Available at: <http://www.ag.gov.au/Publications/Documents/GuideforPractitioners.pdf>.

<sup>17</sup> Law Council of Australia, 'Anti-Terrorism Reform Project: A consolidation of the Law Council of Australia's advocacy in relation to Australia's anti-terrorism measures', June 2012, p. 98. Available at: [http://www.lawcouncil.asn.au/shadomx/apps/fms/fmsdownload.cfm?file\\_uuid=33955F71-1E4F-17FA-D28E-2DB9744044B2&siteName=lca](http://www.lawcouncil.asn.au/shadomx/apps/fms/fmsdownload.cfm?file_uuid=33955F71-1E4F-17FA-D28E-2DB9744044B2&siteName=lca). In fact, and contrary to the Law Council's advocacy report, the section on self-incrimination is not Section 34L but Section 34G Giving information and producing things etc. of the ASIO Organisation Legislation Amendment (Terrorism) Act 2003 (no. 77).

<sup>18</sup> The process of applying for a security clearance in civil cases, as outlined in Section 39A of the NSI Act, in most respects mirrors that followed in criminal cases except that, in light of 'the additional financial burden involved in engaging a security-cleared legal representative to attend a closed hearing, a self-represented litigant...who is refused a security clearance at the appropriate level would be eligible to apply for financial assistance under the Special Circumstances Scheme.' Attorney-General's Department, *National Security Information (Criminal and Civil Proceedings) Act 2004: Practitioner's Guide*, June 2008, p. 42. Available at: <http://www.ag.gov.au/NationalSecurity/Counterterrorismlaw/Documents/Practitioners%20Guide%20to%20the%20NSI%20Act.pdf>. However, consistent with the provisions relating to criminal proceedings, the choice of legal representative is constrained by the need for the nominated representative to have a security clearance at the appropriate level.

<sup>19</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004*, Act No. 150 of 2004 as amended (this compilation including amendments up to Act No. 127 of 2010). Available at: <http://www.comlaw.gov.au/Details/C2011C00375/>.

<sup>20</sup> *NSI Act Practitioner's Guide*, p. 29. This is a claim which, in the absence of evidence of any sort, is neither verifiable nor falsifiable.

<sup>21</sup> *NSI Act*, Section 3 Object of this Act. There is no explanation in the Act itself, or in the *Practitioner's Guide*, as to exactly what 'seriously interfere with the administration of justice' means. Evidently, it is a secret.

<sup>22</sup> This definition of information was inserted into the Criminal Code by the Criminal Code Amendment (Espionage and Related Matters) Act 2002 (Act No. 91 of 2002 as amended). Available at: <http://www.comlaw.gov.au/Details/C2004A01028/>.

<sup>23</sup> *NSI Act Practitioner's Guide*, p. 10.

<sup>24</sup> *Ibid.*

<sup>25</sup> *ASIO Act 1979*, Section 4.

<sup>26</sup> This is not reflected in the order in which the terms appear and are defined in the Act.

<sup>27</sup> *NSI Act*, Section 17. The second part of the definition is as follows: '2. The contravention of a requirement is likely to prejudice national security if there is a real, not merely a remote, possibility that the contravention will prejudice national security.' In the absence of any further explanation, either in the Act itself or the *Practitioner's Guide*, it has to be assumed that 'requirement' refers to something contained in the *Requirements for the Protection of National Security Information in Federal Criminal Proceedings and Civil Proceedings* (otherwise known as the NSI Requirements).

<sup>28</sup> *NSI Act Practitioner's Guide*, p. 17. For more on the NSI Act, including discussion of equivalent legislation in overseas jurisdictions, its provisions for closed court hearings and the issuing of certificates in civil proceedings see Mark Rix, 'Counter-terrorism and information: The NSI Act, fair trials, and open, accountable government', *Continuum: Journal of Media and Cultural Studies*, vol. 25, no.2, 2011, pp. 285-297.

<sup>29</sup> International Commission of Jurists (ICJ), *Assessing Damage, urging action*. Report of the Eminent Jurists Panel on terrorism, counter-terrorism and human rights. Available at:



---

<http://www.un.org/en/sc/ctc/specialmeetings/2011/docs/icj/icj-2009-ejp-report.pdf>. The EJP cites subsection 31(8) of the NSI Act.

<sup>30</sup> Mark Dreyfus, Media Release, 21 March 2013: 'Whistleblower protection introduced to Parliament'. Available at: <http://www.attorneygeneral.gov.au/MediaReleases/Pages/2013/First%20quarter/21March2013-Whistleblowerprotectionintroducedtoparliament.aspx>. The Freedom of Information Act 1982 was reformed in 2010 with the aim being, to use the Government's own rhetoric, to promote a pro-disclosure culture across the government and to build a stronger foundation for more openness in government. The Government also established the office of Australian Information Commissioner and appointed Professor John McMillan to this office. For more on these reforms go to <http://www.ag.gov.au/RightsAndProtections/FOI/Pages/Freedomofinformationreforms.aspx>.

<sup>31</sup> Public Interest Disclosure Bill (first reading), 2013, Division 2 Objects. Bill available at: [http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r5027\\_first-reps/toc\\_pdf/13089b01.pdf;fileType=application%2Fpdf#search=%22legislation/bills/r5027\\_first-reps/0000%22](http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r5027_first-reps/toc_pdf/13089b01.pdf;fileType=application%2Fpdf#search=%22legislation/bills/r5027_first-reps/0000%22). In Division 3, Sections 69 and 70 there is a lengthy list of the office holders who are considered to be public officials, and the agency to which they belong. Curiously, but not surprisingly, the Prime Minister, Speaker of the House of Representatives and ministers, amongst others, are omitted from the list. This means that 'public servants who blow the whistle on wrongdoing by politicians, including concerns about corruption or bribery, would not be protected' under the Bill.' See Matthew Knott, 'Labor's whistleblower bill just window dressing without change', *Crikey*, 26 March 2013. Available at: <http://www.crikey.com.au/2013/03/26/labors-whistleblower-bill-just-window-dressing-without-an-overhaul/>.

<sup>32</sup> *Ibid.* ASIS is Australia's foreign intelligence agency, more correctly Australia's overseas secret intelligence collection agency, and is even more secretive and invisible than ASIO.

<sup>33</sup> *Ibid.* Besides ASIO and ASIS, 'intelligence agency' means the Defence Imagery and Geospatial Organisation, the Defence Intelligence Organisation, the Defence Signals Directorate and the Office of National Assessments.

<sup>34</sup> Suelette Dreyfus, 'Parliament did some work this week: whistleblower bill a milestone', *Crikey*, 28 June 2013 available at [www.crikey.com.au/2013/06/28/parliament-did-some-work-this-week-whistleblower-bill-a-milestone/](http://www.crikey.com.au/2013/06/28/parliament-did-some-work-this-week-whistleblower-bill-a-milestone/)